UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with the account **allcontrol2016@gmail.com**, fully described in Attachment A.

Case No. 19-M-037

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Information associated with the account **allcontrol2016@gmail.com**, fully described in Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 21, United States Code, Sections 829(e), 841(a)(1), 841(h) and 843(c)(2)(A).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Scott Simons
Applicant's signature

DEA Task Force Officer Scott Simons
Printed Name and Title

Sworn to before me and signed in my presence:

Date: April 2, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Scott Simons, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, Inc. ("Google") an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer assigned to the Milwaukee Office of the Drug Enforcement Administration (DEA) as a member of the Tactical Diversion Squad (TDS) specializing in pharmaceutical investigations. I have worked full-time as a Federal Task Force Officer for the past 5 years and a full-time law enforcement officer with the Greenfield Police Department for the past 16 years. During my tenure as a DEA Task Force Officer and a Greenfield Police Department law enforcement officer, I have been involved in the investigation of narcotics traffickers operating not only in the County of

Milwaukee and the State of Wisconsin but also other states throughout the United States. I have received training in the investigation of drug trafficking and computer related crimes. I have worked with informants in the investigations of drug trafficking in the Milwaukee area as well as other jurisdictions within the State of Wisconsin and throughout the United States. I have participated in the application for and execution of numerous search warrants. I have participated directly in numerous narcotics investigations and arrests in which controlled substances and drug paraphernalia were seized. I am familiar with methods that are commonly used by drug dealers to package and prepare controlled substances for sale in various areas.

3. The statements in this affidavit are based on my personal knowledge, information I have received from other law enforcement personnel, publicly available information, and from persons with knowledge of relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation.

4. Based on the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the information associated with the account identified in Attachment A, Google email account **allcontrol2016@gmail.com**, will contain fruits, evidence, and instrumentalities related to violations of Title 21, United States Code, Sections 829(e) and 841(a)(1) (Distribution of Controlled Substances), and Title 21, United States Code, Sections 841(h) and 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet) (the "Subject Offenses"), as further described in Attachment B.

BACKGROUND OF THE INVESTIGATION

5. In February of 2015, the Milwaukee District Office of the DEA initiated an investigation into the internet pharmacy GOLDPHARMA24 located at www.goldpharma-24.com, which advertises for sale controlled and non-controlled pharmaceuticals, including schedule II controlled substances, without requiring a prescription for such substances. During the course of the investigation of GOLDPHARMA24, case agents identified multiple Google and Yahoo accounts used to facilitate the commission of the Subject Offenses. As described below, probable cause exists to believe the Google account associated with the email address identified in Attachment A was used to facilitate the commission of the Subject Offenses.

PROBABLE CAUSE

6. On or about March 21, 2018, case agents from the DEA Milwaukee District Office (MD) applied for and obtained federal search warrants for multiple email accounts for individuals affiliated with the distribution of illegal pharmaceutical products and illegal distribution of controlled substances, including for email address jessicagilmoreph@gmail.com. At the time, case agents believed that email address jessicagilmoreph@gmail.com was utilized by an individual using the alias Jessica Gilmore. However, review of email records related to email address jessicagilmoreph@gmail.com identified the user of the email account as Lucas PAURA, an Argentinean national residing in Buenos Aires, Argentina, who was indicted by a grand jury sitting in the Eastern District of Wisconsin on September 11, 2018 for various drug trafficking offenses.

7. While reviewing the seized email content of email account jessicagilmoreph@gmail.com, case agents identified an email conversation between Alex MATTHEWS (which case agents believe is an alias) and email account jessicagilmoreph@gmail.com that occurred on March 16, 2018, at approximately 7:10 a.m. The email contained a link to a Google Drive URL and a subsequent message stated, "from there you can download your archives." Law enforcement used the URL sent by MATTHEWS to jessicagilmoreph@gmail.com which linked to files saved in a Google drive account. The Google Drive account linked to an individual known only to law enforcement as "Stacey CAMPBELL," which case agents believe is an alias. The URL sent by MATTHEWS linked to files saved in the Google Drive account and did not require a user name or password to access the information contained within the Google Drive account. Based upon their training and experience and their familiarity with the investigation to date, case agents identified multiple documents maintained in the Google drive location that contained information relating to the distribution of controlled substances via illegal internet pharmacies being operated by the GOLDPHARMA24 DTO, including for example, a document listing the employees of the GOLDPHARMA24 call center, and spreadsheets containing drug customer orders.

8. Based on my training and experience, I know that Google Drive allows a Google Drive account holder to share the content of files with others. A Google Drive user does this by sending a URL linked to those files/location to the other party. The files stored in the Google Drive account can then be accessed by clicking on the URL or pasting the URL into a web browser. Depending on users setting, those Google Drive

files are then accessible to anyone who knows the URL. A user accessing the URL is able to view the Google account username for the party sharing the files.

9. During the month of June 2018, case agents interviewed a source of information (SOI) who stated that members of the GOLDPHARMA24 drug trafficking organization utilized a Google Drive account to upload commission files and other documents used by members of the DTO and employees of the call center. The SOI stated that the Google Drive details were sent to members of the organization and the SOI provided law enforcement with the account name of the Google Drive account utilized by members of the GOLDPHARMA24 DTO, including a screenshot of the Google Drive account, which listed the account holder as Stacey CAMPBELL, and the email address as **allcontrol2016@gmail.com**. The SOI stated that after the GOLDPHARMA24 websites were taken offline as a result of an incident in Romania, employees who worked in the GOLDPHARMA24 call center located in Buenos Aires, Argentina, including the SOI, were instructed to contact customers who had previously illegally purchased controlled substances from the GOLDPHARMA24 online pharmacies. The SOI stated that each employee of the GOLDPHARMA24 call center was responsible for accessing the Google Drive account in order to retrieve the contact information for the prior customers that each employee was responsible for contacting. The SOI stated that each member of the call center had their own spreadsheet with the names of customers that had previously purchased illegal pharmaceutical products from the GOLDPHARMA24 organization. Case agents believe the information provided by the SOI to be truthful and reliable because the SOI has provided information regarding the drug trafficking activities of the

GOLDPHARMA24 DTO, which case agents have been able to corroborate through surveillance, controlled buys, and other witness and law enforcement reporting.

10. On August 13, 2018, Google responded to an administrative subpoena requesting basic account information for the email address allcontrol2016@gmail.com. The email account was created on May 17, 2016, at approximately 19:29:48-UTC from IP address 158.69.133.62. The Google account services accessed by this account were: Android, Blogger, Chrome Web Store, Gmail, Google AdWords, Google Analytics, Google Calendar, Google Docs, Google Drive, Google Hangouts, Google My Maps, Google Play Music, Google Search Console, Location History, Web & App Activity, and YouTube. A telephone number of +5491125134861 was listed as the SMS number on the account. Case agents are aware that GOLDPHARMA24 operates a physical call center located in Buenos Aires, Argentina and this telephone number is consistent with a telephone number located in the City of Buenos Aires, Argentina.

11. Throughout the course of this investigation, case agents have confirmed that members of the GOLDPHARMA24 DTO utilized aliases and fictitious names to create email accounts and phone accounts in an attempt to mask their illegal criminal activity while operating online. Based upon their training and experience and the investigation to date, case agents believe that the name "Stacey Campbell" and "Alex Matthews" are fictitious names created for the purpose of masking the illegal criminal activity committed by members of the GOLDPHARMA24 drug trafficking organization.

12. On October 31, 2018, the Honorable William E. Duffin, United States Magistrate Judge for the Eastern District of Wisconsin, signed a federal search warrant

for **allcontrol2016@gmail.com**. Case agents received email account records for the aforementioned email account pursuant to this search warrant. Case agents subsequently reviewed these records and found numerous files saved within the Google Drive documenting the illegal distribution of controlled and non-controlled prescription pharmaceuticals primarily to customers located in the United States. These files documented details including, but not limited to, the customer's name and address, drug type, drug quantity, and amount paid by the customer.

13. On March 12, 2019, Argentine law enforcement officials, including officers from the Buenos Aires City Police Department, along with case agents, executed multiple search warrants at locations associated with the GOLDPHARMA24 DTO, including the call center. On March 12, 2019, three members of the GOLDPHARMA DTO who were indicted in the Eastern District of Wisconsin were arrested in Buenos Aires. Case agents interviewed GOLDPHARMA24 call center employees, all of whom were out of custody and provided voluntary statements to case agents at the U.S. Embassy located in Buenos Aires, Argentina. All of the GOLDPHARMA24 call center employees interviewed stated that the files containing a list of all customer orders were saved in a Google Drive account that the DTO. The GOLDPHARMA24 call center employees did not recall the specific Gmail account associated with the Google drive, but they did say the profile photograph was of the television show The Simpsons. Case agents are aware that the profile photograph for **allcontrol2016@gmail.com** is that of The Simpsons television show. Case agents believe that the Google Drive for **allcontrol2016@gmail.com** will contain updated customer orders since the execution of the search warrant on October 31, 2018, and that

the customer orders will have ended on or about March 12, 2019, which is the day the DTO was dismantled.

BACKGROUND CONCERNING GOOGLE

14. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain a free email account at the domain name gmail.com like the Subject Account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information.

15. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying

subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

18. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

19. In addition to email, Google offers its users a number of other online services. A list of those services and their feature is available at the following URL: https://support.google.com/.

20. As described above, one of the services Google offers is Google Drive. As discussed above, Google Drive is a file storage and file sharing application that allows its users to share access to the content of files by sending a URL to others. According to information available from Google, Google stores the content of those files on their servers.

21. In my training and experience, and publicly available information from Google, I know that Google uses cookies and similar technology to collect information about its users, including to identify a user's device and browser version. Google also states that it uses "technologies" to determine a user's actual location.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2713 by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

23. Based on the information described above, I request that the Court issue the proposed search warrant for the Subject Account.

24. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the account **allcontrol2016@gmail.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 (the "Provider").

ATTACHMENT B

Particular Things to be Disclosed and Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 18, 2019, the Provider is required to disclose the following information to the government for each of the accounts or identifiers listed in Attachment A:

a. All customer information (e.g. name, age, email address, physical address, payment information) associated with the account;

b. All records and information regarding the creation account and access to the account, including records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, and log-in IP addresses associated with session times and dates.

c. The types of services utilized;

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

e. All records, files, and other information stored/saved in the accounts, including information, files, and data saved to Google Drive;

f. A complete file activity log for any associated Google Drive account;

g. All records and information and analytics collected by the Provider through the use of cookies or similar technology including the type of browser and device used by the account holder, the web page visited before coming to Google sites, and other identifiers associated with the devices used by the account holder;

h. All records and information that identifies a user's actual location;

i. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken;

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of the warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities related to violations of Title 21, United States Code, Sections 829(e) and 841(a)(1) (Distribution of Controlled Substances), and Title 21, United States Code, Sections 841(h) and 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet), since October 31, 2018, including but not limited to, information pertaining to the following matters:

a. Information identifying the persons using the account;

b. Information identifying other accounts used by the persons using the account;

c. Information identifying the devices used to access the account;

d. The location of persons using the account;

e. The identity of persons sharing Google Drive account URLs associated with the account;

f. The identity of persons saving, storing, editing, and accessing files and records on Google Drive accounts associated with the account;

g. Financial information, credit card numbers, social security numbers, and other personal identifiable information stored in the Google Drive account;

h. Information related to the sale and distribution of controlled substances and pharmaceuticals; and

i. Communications and files that contain IP addresses and username and passwords to those IP addresses.